

Exhibit 2

Expert Disclosure – Philip A. Werlau
(March 12, 2025)

Philip A. Werlau is a Senior Investigator at Anchian.AI. This testimony is disclosed in rebuttal to the defendant's expert disclosures, and the Government reserves the right to present this testimony in its case in chief or in its rebuttal case at trial.

A. Anticipated Opinions

Outlined below are the rebuttal opinions that Mr. Werlau is expected to offer as well as the bases and reasons for those opinions:

1. In response to paragraph 42 of the Edman disclosure, the description of the proxy contracts contained therein is incomplete and omits important detail about how the overall architecture of the Tornado Cash service worked together. In particular, the Tornado Cash Router contract was the starting point for deposits and withdrawals using both the UI and the CLI after it was deployed in or around February 2022, as discussed in Mr. Werlau's opening disclosure. The Router, in concert with the Instance Registry, could have been updated during the time period charged in the Indictment to disable these smart contracts' ability to interact with the Tornado Cash pools. This would have prevented customers from accessing the Tornado Cash pools through the Tornado Cash UI or CLI. This testimony will be based on the code for the UI, the CLI, and the relevant smart contracts.

2. In response to paragraph 51 of the Edman disclosure, Mr. Werlau will explain that the UI and CLI for the Tornado Cash service determined which smart contract to interact with to execute deposits and withdrawals for customers. In fact, the UI and CLI were periodically updated to replace the old "proxy" contract with a new "proxy" contract, including when the Tornado Cash Router was created. Accordingly, the individuals who controlled the UI and CLI—that is, the three Tornado Cash founders—had the ability to create a new "proxy" smart contract to replace the Tornado Cash Router smart contract at any time, and without waiting for a proposal or vote from the Tornado Cash Governance smart contract. This would have enabled the founders to unilaterally implement a sanctions screening mechanism, including but not limited to the Chainalysis Oracle or a know-your-customer mechanism as described in Mr. Werlau's original proposal, into the transactional architecture of the Tornado Cash service rather than simply at the UI level.

3. In response to paragraph 54 of the Edman disclosure, Mr. Werlau provides the following additional information about his methodology. To attribute transactions to the UI or CLI, Mr. Werlau applied the methodology set forth in more detail in the document titled "Gas Analysis Methodology" that is being produced along with this disclosure. As explained in that document, this methodology included simulating thousands of deposits using Foundry's anvil software, custom code matching the relevant deposit code from the period of the deposit, and an Infura RPC endpoint. A spreadsheet identifying which transactions were attributed to the UI, CLI, or other is being produced along with this disclosure. This spreadsheet reflects slight revisions from the prior spreadsheet produced with Mr. Werlau's original disclosure, but the overall approximate percentages identified in that prior disclosure remain the same. Mr. Werlau also checked his methodology by reviewing certain Tornado Cash deposits where the person making

the deposits has informed the Government that he used the UI, and confirmed that these deposits were attributed to the UI by his methodology. This testimony will be based on blockchain data, and the code for the versions of the UI and CLI that existed at different points during this time period.

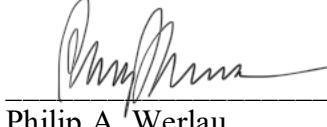
4. In response to paragraph 13(c) of the Hurder disclosure, Mr. Werlau analyzed the code for the Tornado Cash user interface and determined that the code did not work as described in the Hurder disclosure. Specifically, while it is correct that in general, the relayer algorithm increased a relayer's chance of being selected as the relayer's fee went down, that was only true up to a point. The relayer algorithm provided no incentive for reducing relayer fees below a minimum set in the code for the algorithm, which in practice worked as a functional floor on the amount of the fee that relayers were likely to charge and did charge. From on or about March 23, 2022 onward, this minimum was set at a relayer fee of 0.33% of the withdrawal amount. This testimony will be based on the computer code for the user interface.

5. In response to paragraph 15 of the Hurder disclosure, Mr. Werlau analyzed blockchain data for withdrawals from the Tornado Cash service on the Ethereum blockchain from March 1, 2022 through August 8, 2022. A summary of that data is being produced along with this disclosure. That analysis reveals that more than 99% of withdrawals during this time period used a relayer. Of that 99%, approximately 5% can be classified as self-relayed withdrawals, in which a customer entered the same address as the relayer and the withdrawal address when making a withdrawal. Those are excluded from this analysis. Of the remaining relayed withdrawals, which constitute approximately 94% of all Tornado Cash withdrawals from this time period, approximately 99% used a relayer that had at one point staked enough TORN tokens to be included in the Relayer Registry. Additionally, while it would be possible for a customer to use a relayer who had not staked TORN tokens to be included in the Relayer Registry, in practice this would have required multiple steps for the customer to identify such a relayer for each withdrawal, and would have significantly reduced the ease of use of the Tornado Cash service for the typical customer. This testimony will be based on blockchain data and the code for the UI.

6. In response to paragraph 15(g) of the Hurder disclosure, Mr. Werlau looked at the description of the commissions paid by relayers to the User Vault in Tornado Cash documents, including the March 1, 2022 announcement of the relayer network and Relayer Registry. These materials describe these commissions as "staking rewards," indicating that the design of the system was meant to enable TORN token holders to have the option of receiving a share of the relayer commissions by staking TORN tokens in the Governance contract. Additionally, based on blockchain data for the period from March 2022 through August 8, 2022, the relayer commissions were in fact distributed to TORN token holders and were not used for other purposes. Thus, while it was technically possible for the TORN token holders with staked tokens to vote to use these commissions for other purposes, in practice these commissions were a form of profit to TORN token holders who staked in the governance contract. This testimony will be based on documents prepared by the founders and operators of the Tornado Cash service, on the code for the relevant smart contracts, and on blockchain data.

B. Approval and Signature

I hereby approve the disclosure of my qualifications, anticipated opinions, and bases for such opinions, as set forth above.



Philip A. Werlau